

DATA SHARING ACT 2025 AND THE CONSTITUTIONAL SAFEGUARDS ON INFORMATIONAL AUTONOMY IN MALAYSIA

SITI SUMAYYAH MUSA^{1*}, FARID SUFIAN SHUAIB²,
SONNY ZULHUDA³

^{1,2,3} Ahmad Ibrahim Kulliyah of Laws, International Islamic University Malaysia, Gombak, Malaysia

*Corresponding author: thareeq09@gmail.com

ABSTRACT: Malaysia's rapid digitalisation of public administration has significantly expanded the scale and intensity of personal data processing within government digital services. Platforms such as MySejahtera, PADU, MyIdentity, MyDigital ID and one stop centre MyGov apps have become central to service delivery, policy implementation, and data-driven governance. The new Data Sharing Act 2025 (DSA 2025) is a significant piece of legislation designed to facilitate inter-agency data sharing and enhance administrative efficiency. However, the centralisation and dissemination of personal data within the public-sector raise important constitutional and governance questions concerning informational autonomy and state accountability. Although the Federal Constitution does not expressly recognise a right to privacy, Malaysian courts have interpreted Article 5 (1) on life and personal liberty, together with Article 8(1) on equality before the law, as comprising elements of autonomy, dignity, and protection against arbitrary state action. This paper adopts a doctrinal legal methodology to examine whether the institutional design and operational mechanisms of the DSA 2025 adequately align with these constitutional principles. It analyses the Act's data-sharing architecture, executive discretion, and oversight arrangements, and evaluates the extent to which existing constitutional safeguards constrain state power over the processing of citizens' personal data. Drawing on comparative insights from Germany, the European Union, the United Kingdom, and Canada, the paper argues that effective public-sector data governance requires principles constraints that extend beyond administrative efficiency. It proposes the development of a Malaysian Doctrine of Informational Autonomy, grounded in Articles 5(1), 8(1), and constitutional supremacy, to provide a coherent framework for assessing the constitutional and governance-based analytical framework, this paper contributes to ongoing debates on digital governance, trust, accountability, sovereignty and the protection of individual informational liberty in Malaysia's evolving data-driven services.

KEYWORDS: Governance, Digital Services, Constitutionalism, Personal Data

1. INTRODUCTION

Malaysia's rapid transition towards a data-driven public administration has significantly expanded the scale and complexity of personal data processing within government digital services (Nisar et al, 2025). Public sector platforms such as

MySejahtera, *PADU*, *MyDigital ID*, and *MyIdentity* have become central infrastructures for delivering services, managing entitlements, and facilitating data-driven policy changes. In an increasingly interconnected governance ecosystem, these approaches increase administrative efficiency but also raise questions about state accountability, autonomy, and informational privacy. In light of this, the Data Sharing Act 2025 (DSA 2025), which aims to support national digitalisation goals while streamlining cross-agency data access, represents a significant regulatory development. However, the significant concerns about sovereignty, constitutional protections and the boundaries of state authority over personal data are raised by the centralisation and sharing of personal data among public-sector government agencies (Harun, 2025).

The Federal Constitution does not explicitly recognise a right to privacy. However, as demonstrated most notably in *Sivarasa Rasiah v Badan Peguam Malaysia* [2010] 2 MLJ 333, Malaysian courts have construed Article 5(1), which protects the right to life and personal liberty, as containing aspects of autonomy, dignity, and personal privacy (Hashim, 2020). A purposive interpretation of fundamental liberties has been upheld by later case law, such as *Maria Chin Abdullah v Ketua Pengarah Imigresen & Anor* [2021] MLJU 12 and *CTEB & Anor v Ketua Pengarah Pendaftaran Negara, Malaysia & Ors* [2020] 3 MLJ 634, which highlights a wider evolution of the constitution. However, the courts have not established a unified standard governing informational privacy or constitutional bounds of state data operations, and these legal developments continue to be scattered. The implementation of DSA 2025, which permits significant interagency data exchange without commensurate constitutional standards of need, proportionality, or non-arbitrariness, shows this doctrinal gap.

The inherent power imbalance between the State and the citizen is worsened by the growth of government data infrastructure, posing structural issues that cannot be resolved by administrative or legal means alone (Oskar.JG, 2023). Strong data governance frameworks must be based on constitutional principles that limit the discretionary use of public power, as shown by comparative jurisdictions such as Canada's constitutionalised oversight of government data handling, the United Kingdom's public-sector data protection regime, and Germany's Informational Self-Determination doctrine. According to these models, constitutional protections that guarantee openness, accountability, and the preservation of individual right must be balanced with statutory efficiency.

Therefore, this paper suggests that DSA 2025 lacks the constitutional protections required to control the State's increased authority over personal data, even as it fosters digital governance (Daud. M, 2025). Due to the Act's focus on administrative effectiveness and interoperability, constitutional standards that are often applied to protect individual right are not clearly included. Malaysia needs a coherent constitutional doctrine in the absence of an explicit right to privacy in order to provide assurance that public-sector actions involving personal data adhere to the rule of law, refrain from arbitrary intrusion, and respect individual liberty.

Thus, based on Article 5(1) and Article 8(1) of the Federal Constitution as well as the idea of constitutional supremacy, this paper recommends Malaysia to develop a stand-alone Malaysian doctrine of informational autonomy (Hongqiang.Z et al, 2025). Such concept would guide judicial interpretation, harmonise statutory

instruments with fundamental liberties, and offer a clear analytical framework for assessing the constitutionality of government data actions. Malaysia may better integrate its digital transformation strategy with the protection of civil liberties and the long-term validity of the constitutional order by establishing data governance on constitutional principles rather than emphasising chiefly on administrative expediency.

2. MALAYSIA'S CONSTITUTIONAL FRAMEWORK ON STATE POWER AND PERSONAL DATA

Malaysia's Federal Constitution does not expressly recognise a right to privacy. This absence is textual and can be confirmed by examining the Constitution's provision, which do not include "privacy" as a fundamental liberty. Article 5 (1) guarantees that "No person shall be deprived of his life or personal liberty save in accordance with law", Scholars and courts have interpreted "personal liberty" as extending beyond physical restraint to include facets of autonomy and dignity. The precise doctrinal scope of autonomy under Article 5 (1) has not been definitely settled by the courts.

In *Sivarasa Rasiah v Badan Peguam Malaysia* [2010] 2 MLJ 333 the Federal Court held that Article 5 (1) encompasses rights implicit in "life" and "personal liberty", provided that they are consistent with the Constitution. This case is commonly read to imply that informational or decisional autonomy may fall within the ambit of Article 5 (1), although the Court did not explicitly address digital privacy. In *Maria Chin Abdullah v Ketua Pengarah Imigresen & Anor* [2021] MLJU 12, the High Court applied a purposive reading of Article 5 (1), emphasizing evolving societal contexts. Thus, this demonstrates judicial willingness to interpret fundamental liberties dynamically, though not specifically in the context of government data practices. In *CTEB & Anor v Ketua Pengarah Pendaftaran Negara, Malaysia & Ors* [2020] 3 MLJ 634, the court adopted a more flexible constitutional approach, departing from strict literalism. Therefore, despite the lack of a clear privacy concept, this provides validity to the idea that Malaysian constitutional jurisprudence may adjust to new technological realities.

The Federal Court's broad interpretation of the right to personal liberty had been referred to in some other cases, all giving more favour and support to the acceptability of right to privacy as a constitutional right in Malaysia (See, for example, *Toh See Wei v Teddric Jon Mohr & Anor* [2017] 4 AMR 903; *Pendakwa Raya Iwn Nor Hanizam bin Mohd Noor* [2019] MLJU 638, HC and *Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors* [2022] 11 MLJ 898, HC). But despite this decision, the right to receive a civil remedy on the basis of invasion of privacy may still be far from settled.

2.1. State Power and Absence of Explicit Data Protection Duties

Government agencies are exempted from the Personal Data Protection Act 2010 (PDPA) [Act 709] under Section 3 (1). As a result, rather than extensive statutory obligations, the State's handling of personal data is generally governed by administrative policy and sector-specific legislation. As of right now, Malaysia lacks

a comprehensive constitutional or statutory concept that establishes restrictions on the gathering, use, and dissemination of government data. Meanwhile, interagency data exchange procedures are introduced by the DSA 2025. Although the Act increases executive power over data flows, it does not include clear constitutional requirements for minimal impairment, necessity, or proportionality.

Article 8(1) of the Federal Constitution guarantees that “all persons are equal before the law and entitled to the equal protection of the law.” This principle of non-arbitrariness is commonly derived from Article 8 (1), and courts have applied this principle to strike down arbitrary state action. In the context of government data practices, arbitrary or disproportionate data collection or sharing may implicate Article 8 (1), although no case yet addressed this directly.

2.2. Constitutional Supremacy and Digital Governance

Article 4(1) establishes that the Federal Constitution is the supreme law of the Federation. Any statute including the DSA 2025 must therefore comply with constitutional standards governing personal liberty and equality. Constitutional supremacy is upheld by Malaysian courts, although previously untested, they usually require a definite disagreement between statute and constitution before declaring legislation unconstitutional (Hamid. N, 2019).

The Data Sharing Act 2025 (DSA 2025) [Act 864] of the Parliament of Malaysia. The Act was gazetted on 20 February 2025 and came into force on 28 April 2025. The long title of the Act states that it provides for the sharing of data under the control of a public sector agency with other public-sector agencies, the establishment of the National Sharing Committee, the functions and powers of the Director General of the National Digital Department in relation to data sharing, and related matters.

Official explanatory materials and FAQs issued by the National Digital Department describe three main objectives of the DSA 2025:

- (i) To provide clear legal authority to regulate and enforce laws related to data sharing;
- (ii) To improve the effectiveness of data sharing implementation and management among agencies; and
- (iii) To establish a more systematic and focused governance structure within the data sharing ecosystem.

Section 2 of the Act states that it binds the Federal Government. The official FAQ clarifies that the Act applies to data under the control of federal public sector agencies and federal statutory bodies, and that its scope is confined to the federal government machinery. Consequently, state governments and state-level entities fall outside the direct scope of the Act unless separately brought within its regime.

The Act defines, in Section 3 “public-sector agency” to include the public services under Article 132 (1) of the Federal Constitution (with specified exclusions) and statutory authorities exercising powers vested by federal law. This definition positions the DSA 2025 as an internal federal data-sharing framework, rather than a law directly directed at private-sector actors. In addition, the Act defines “data”

broadly as any facts, statistics, instructions, concepts or other information capable of being communicated, analysed or processed by individuals, computers or other means. This definition clearly extends beyond “personal data” as understood in the Personal Data Protection Act 2010 (PDPA), thereby covering both personal and non-personal information within the public-sector.

Commentaries note that the DSA 2025 framework may indirectly affect private entities where they are engaged by public agencies to perform data migration, data integration or data analytics work, and in such cases those entities must comply with the Act’s security and handling requirements. Although the Act does not directly reconfigure private-sector obligations under the PDPA, it creates a secondary layer of compliance for private contractors working with public-sector data.

2.3. Institutional Structure: National Data Sharing Committee and the Role of Director General

Part II of the Act establishes a National Data Sharing Committee (the Committee). The Committee is chaired by the Minister responsible for digital affairs and includes, among others, representatives from each ministry, the Prime Minister’s Department, the Chief Government Security Officer, the National Cyber Security Agency (NACSA), and the Personal Data Protection Department. Section 6 (1) sets out the Committee’s functions, which include: formulating policies and strategies on data sharing; overseeing implementation of the Act; resolving administrative difficulties; formulating policies relating to databases for data sharing; and performing necessary consequential functions. The Committee is therefore designed as a central policy and coordination body with substantial influence over the architecture of public-sector data governance.

Section 11 of the Act confers specific duties and powers on the Director General of the National Digital Department, including: implementing Committee policies; coordinating and facilitating data sharing; advising the Committee; requiring information or documents; issuing circulars or guidelines; and carrying out other duties as directed. This places the Director General in a pivotal operational role, effectively functioning as the executive authority for the day-to-day administration of federal data sharing.

Part IV of the DSA 2025 regulates the process by which a public sector agency may request data from another public sector agency. Section 12 provides that a requesting agency must specify, among others, (a) the data requested; (b) the purpose for which the data is requested; (c) the public sector agencies that will act as data provider and data recipient; and (d) the manner in which the data will be handled. Commentaries describe that the receiving agency must evaluate the request against statutory criteria, including relevance to the stated purpose, consistency with Section 13 of the Act, and risks to health, safety, welfare or other protected interests. This indicates an internal administrative gatekeeping process that purports to structure inter-agency data flows.

The Act states that it is to be read together with other written laws that allow data sharing and that its provisions are “in addition to, and not in derogation of,” the relevant written laws. This “pillar” clause, prescribed in Section 4, suggests that the DSA 2025 is intended to overlay existing sectoral frameworks rather than displace

them. The Act expressly provides that data of public sector agencies must be dealt with in accordance with the Official Secrets Act 1972 and other specified laws listed in the Schedule, and that disclosures under the DSA 2025 are deemed to be disclosures under those laws. This provision is significant because it normalises internal data disclosures by situating them within existing secrecy and confidentiality regimes.

2.4. Constitutional Risks Posed by the Data Sharing Act 2025

The DSA 2025's institutional structure, which places operational authority in the Director General of the National Digital Department and policy-making in the National Data Sharing Committee, tend to concentrate decision-making power within the executive branch. The main control over data flows is administrative rather than constitutional or judicial since requests and authorisation for data sharing are managed internally amongst public-sector entities, with appraisal carried out by other executive actors (Harun, 2025). From the perspective of Article 5(1) of the Federal Constitution, such concentration of discretion over citizens' data raises the risk that interagency sharing may affect aspects of personal liberty without being subjected to an explicit necessity or proportionality test.

As discussed earlier, the Personal Data Protection Act 2010 (PDPA 2010) does not extend to the Federal Government or State Governments pursuant to section 3(1). By contrast, the Data Sharing Act 2025 (DSA 2025) is designed to operate within the public-sector context, including federal entities that are not subject to any comprehensive personal data protection regime. As a result, the data-sharing mechanisms established under the DSA 2025 may operate within a less stringent regulatory framework than that applicable to personal data processing in the private sector. This structural divergence raises legitimate concerns regarding the adequacy of data privacy safeguards for citizens.

Nevertheless, this risk may be mitigated, at least in part, by the statutory duty imposed under the DSA 2025 on all parties involved in data sharing in which both data providers and data recipients to take the necessary measures to safeguard the security and privacy of shared data (Section 16(b) DSA 2025). This duty encompasses, *inter alia*, the protection of data from loss, misuse, unauthorised or accidental modification, access or disclosure, alteration, or destruction in language that closely mirrors the security principle under the PDPA 2010, as well as the preservation of individuals' rights relating to personal data protection. However, in the absence of further statutory elaboration or interpretive guidance on the scope and content of these "rights," it remains uncertain how this obligation will operate in practice, particularly in relation to the protection of citizens' data privacy and informational autonomy.

3. INFORMATIONAL AUTONOMY AND LOSS OF INDIVIDUAL CONTROL

The concepts of dignity and personal liberty that Malaysian courts have linked to Article 5 (1) are intimately linked to informational autonomy, which is defined as an individual's ability to govern the disclosure and use of personal data. Under the

DSA 2025 framework, individuals whose data are collected by one public sector agency typically have no direct procedural role in authorising or refusing subsequent inter-agency sharing.

Article 8(1) guarantees equality before the law and equal protection of the law. When large volumes of data are pooled and analysed across agencies, there is a heightened possibility that algorithmic profiling, risk scoring, or categorization may be used to shaped how services, enforcement, or benefits are distributed. In the absence of explicit statutory duties to conduct equality or non-discrimination assessments before deploying data-driven decision systems, there is a constitutional risk that data sharing may indirectly lead to practices that conflict with Article 8(1).

3.1. Transparency, Accountability, and Rule of Law Concerns

Article 4(1) declares the Federal Constitution to be the supreme law of the Federation. Constitutional supremacy presupposes that exercises of public power are sufficiently transparent and reviewable so that courts, Parliament, and the public can assess their legality and compatibility with fundamental liberties (Widiarto et al., 2025). It is unclear to what extent data-sharing agreements, internal policies, or risk assessments made under the Act are published or systematically tabled before Parliament. Limited transparency regarding the exact scope, frequency, and purposes of inter-agency data exchanges makes it difficult for individuals to know when their information has been shared and on what legal basis. This lack of visibility can weaken the practical operation of the rule of law, because individuals may be unable to identify specific decisions or practices to challenge in court under Article 5(1) or 8(1). When considered collectively, these characteristics point to a structural conflict between the DSA's efficiency-driven reasoning and the constitutional need that state power exercises that impact equality and individual liberty be subject to clear, debatable, and moral restraints.

The foregoing analysis indicates that the constitutional risks posed by the DSA 2025 are systemic rather than episodic: they arise from the overall architecture of data sharing rather than from isolated breaches or misuse. At the level of Article 5(1), the main risk is that broad administrative discretion over personal data could compromise liberty and autonomy without being held to the unambiguous constitutional requirements of proportionality and necessity. At the level of Article 8(1), the risk lies in opaque, data-driven decision-making that may result in unequal treatment or hidden forms of discrimination that are difficult to trace and contest. At the level of Article 4(1) and the rule of law, concerns focus on the limited transparency and external oversight mechanisms governing how public sector agencies design, authorize, and implement cross-agency data flows. These combined risks support the central claim of this paper, that Malaysia would benefit from a structured Doctrine of Informational Autonomy to guide legislative design and judicial review of public sector data sharing, ensuring that digital governance remains anchored in constitutional principle rather than administrative expediency (Sukerta et al, 2024).

4. COMPARATIVE DOCTRINES: TOWARDS INFORMATIONAL AUTONOMY

4.1. Germany: Information Self-Determination

The German Federal Constitutional Court, in its 1983 Census decision, recognized a fundamental right to informational self-determination under the German Basic Law. The Court grounded this right in Article 2 (1) (general freedom of action) read with Article 1(1) (human dignity) of the Basic Law. Informational self-determination has been described as granting individuals the authority to decide, in principle, when and within what limits personal data may be disclosed and used (Vladimirovna, 2022).

This doctrinal move constitutionalised control over personal data as a dimension of personal freedom and dignity rather than treating it merely as a statutory or administrative concern. Commentators note that the 1983 Census judgment laid the foundations of both constitutional and sub-constitutional German data protection law. The decision established several requirements for legislation that restricts informational self-determination, including clear legal basis, specific purposes, necessity, and proportionality (Roßnagel et al, 2025).

In practical terms, this means that German public authorities must justify large-scale data collection and linkage by reference to constitutionally acceptable aims and must ensure that risks of profiling, misuse or chilling effects are mitigated.

For Malaysia, the German experience illustrates how a court-developed doctrine can supply a coherent constitutional framework for evaluating state data practices, even in the absence of explicit textual reference to “privacy” or “data protection”.

4.2. European Union: Fundamental Right to Data Protection

The EU Charter of Fundamental Rights recognises a distinct right to the protection of personal data in Article 8, separate from the right to respect for private and family life in Article 7. Article 8(1) states that “Everyone has the right to the protection of personal data concerning him or her.” Article 8(2) further requires that such data be processed fairly for specified purposes and on the basis of consent or another legitimate legal basis, and that individuals have rights of access and rectification. Article 8(3) stipulates that compliance with these rules shall be subject to control by an independent authority. The General Data Protection Regulation (GDPR) is widely described as the key legislative instrument that operationalises this fundamental right to data protection in EU law. The EU model therefore combines an explicit constitutional right, detailed legislative standards, and independent supervisory authorities as core pillars of its data-protection architecture. For public-sector data processing, including inter-agency sharing, the GDPR’s requirements, such as purpose limitation, data minimisation, legal basis, and data subject right, serve as enforceable constraints on state power (Legido-Quigley et al, 2025).

Compared with Malaysia, where constitutional privacy is implied and public-sector data protection duties are scattered, the EU framework represents a more explicit and vertically structured regime in which constitutional, legislative and institutional safeguards mutually reinforce each other.

4.3. United Kingdom: Public-Sector Data Protection Under UK GDPR and The Data Protection Act 2018

In the United Kingdom, data protection is governed primarily by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). Government guidance states that the UK's data protection legislation controls how personal information is used by organisations, including government departments. The DPA 2018 is described as the UK's national data protection law that supplements UK GDPR and applies to organisations processing personal data in the UK, including the public-sector (Lim, 2025).

The Information Commissioner's Office (ICO) is identified as the independent authority responsible for regulating and enforcing UK GDPR and the DPA 2018, including in relation to government bodies. This institutional design ensures that public-sector data practices are subject to an external regulator with investigative and enforcement powers, including the ability to issue guidance, conduct audits, and impose sanctions.

UK GDPR and the DPA 2018 collectively impose legal duties on public authorities, such as lawfulness, fairness, transparency, purpose limitation, accuracy, storage limitation, and integrity and confidentiality, which constrain inter-agency data sharing. Although the UK does not have a written constitution comparable to Malaysia's, the statutory regime operates as a functional equivalent to a constitutional safeguard in the specific domain of data protection, particularly when combined with judicial review and human rights instruments.

For Malaysia, the UK example highlights how even without an entrenched constitutional right to data protection, robust public-sector data governance can be achieved through comprehensive legislation and an empowered independent regulator, elements currently missing from Malaysia's treatment of government-held personal data.

4.4. Canada: Privacy Act and Federal Public-Sector Data Governance

At the federal level in Canada, the Privacy Act (R.S.C, 1985, c.P-21) governs the collection, use and disclosure of personal information by federal government institutions. Section 2 of the Privacy Act states that its purpose is to extend the laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information (Desrochers, 2024).

Official explanations emphasise that the Privacy Act applies to how the federal government collects, uses and discloses personal information, and that it gives individuals the right to access and request correction of their personal information held by government institutions. The Act is administered by the Privacy Commissioner of Canada, who has oversight functions including investigating complaints and reporting to Parliament. As a result, Canadian federal public-sector data practices are structured by a rights-based statute that both limits government handling of personal information and provides individuals with enforceable procedural mechanisms. The combination of statutory privacy rights, access and

correction mechanisms, and independent oversight enables individuals to challenge or scrutinise federal inter-agency data sharing, even where there is no explicit constitutional text equivalent to Article 8 of the EU Charter.

For Malaysia, the Canadian model underscores the importance of having a dedicated public-sector privacy statute that sits alongside, and complements, any private-sector data protection framework, something currently absent given the PDPA's exemption for government.

4.5. Lessons for Doctrine of Informational Autonomy in Malaysia

Across Germany, the EU, the UK and Canada, a common pattern is observable: public-sector data practices are constrained by a combination of (i) rights or rights-like principles, (ii) comprehensive legislative frameworks, and (iii) independent oversight institutions.

Germany exemplifies a court-created constitutional doctrine (informational self-determination), which then shapes legislation and administrative practice. The EU model embeds data protection as a constitutional fundamental right, operationalised through the GDPR and supervised by independent authorities in each Member State.

The UK and Canada illustrate statutory-rights models in which detailed legislative obligations and independent regulators perform a function analogous to constitutional safeguards in the specific area of data protection. In contrast, Malaysia's framework for public-sector data governance currently lacks all three elements in a fully developed form: there is no explicit constitutional right to data protection, no comprehensive public-sector data protection statute, and no independent authority with a clear mandate over government data practices.

The comparative experience therefore supports the central claim of this paper that Malaysia would benefit from articulating a Doctrine of Informational Autonomy, grounded in the existing text and structure of the Federal Constitution but informed by foreign models (Abdul Hadi et al, 2024).

Such a doctrine would not need to replicate any particular foreign system wholesale; rather, it could adapt the core ideas of autonomy, proportionality, transparency, and independent oversight into a framework compatible with Malaysia's constitutional arrangements and institutional context.

5. TOWARDS A MALAYSIAN DOCTRINE OF INFORMATIONAL AUTONOMY

5.1. Constitutional Foundations

Article 4(1) of the Federal Constitution declares the Constitution to be the supreme law of the Federation. Article 5 (1) guarantees that no person shall be deprived of life or personal liberty save in accordance with law. Article 8 (1) provides that all persons are equal before the law and entitled to the equal protection of the law. Read together, these provisions establish that any statutory framework which authorises the State to collect, process, and share personal data must remain

subject to constitutional limits on arbitrariness and unjustified interferences with liberty and equality.

Existing Malaysian case law, including *Sivarasa Rasiah*, *Maria Chin Abdullah* and *CTEB*, indicates that the courts are willing, at least in principle, to interpret fundamental liberties purposively and in light of contemporary conditions. The courts have not yet explicitly framed informational privacy or data protection as a distinct constitutional right. However, the recognition that “life” and: “personal liberty” encompass more than mere physical restraint suggests a conceptual space within which a doctrine of informational autonomy could be developed without constitutional amendment.

A Malaysian Doctrine of Informational Autonomy would therefore operate as an interpretive framework derived from Article 5(1), 8(1) and 4(1), guiding both judicial reasoning and legislative design in matters involving State control over personal data.

5.2. Core Elements of the Proposed Doctrine

The proposed Malaysian Doctrine of Informational Autonomy can be structured around five core elements: autonomy, justification, proportionality, transparency, and accountability and redress (Abdul Halim et al, 2018) (Ong, 2020), (Sweet & Mathews, 2017) & (Abdul Hadi, 2024).

- i. **Autonomy** - First, the doctrine should recognise that personal data not merely administrative resources but are closely linked to individual autonomy, dignity, and self-development. Informational autonomy, in this sense, refers to the individual’s interest in controlling, within reasonable limits, the disclosure, use, and onward circulation of personal data held by public authorities. his recognition does not require an absolute veto for individuals over all forms of public-sector data processing but does require that State decisions affecting personal data be treated as interferences with liberty that demand principled justification (Abdul Hadi, 2024).
- ii. **Justification and Necessity** -Second, the doctrine should require that any significant collection, aggregation, or sharing of personal data by the State be supported by a clear and legitimate purpose grounded in law. For public-sector data sharing under the Data Sharing Act 2025, this would mean that agencies must be able to show that the requested data are genuinely necessary to achieve a specified statutory of policy objective, rather than merely convenient. The doctrine would encourage courts, when reviewing such measures, to ask whether less data-intensive means was reasonably available to achieve the same ends (Abdul Halim et al, 2018).
- iii. **Proportionality and Minimal Impairment**- Third, the doctrine should incorporate a proportionality requirement, under which the scope and intensity of data sharing must be proportionate to the importance of the objective pursued. This entails consideration of the breadth of data categories shared, the number of agencies involved, the duration of retention, and the potential downstream uses of the data. A minimal impairment principle would require that inter-agency data flows be designed

- to minimise unnecessary exposure of sensitive attributes and to limit secondary uses unrelated to the original purpose (Harun, 2025).
- iv. **Transparency**- Fourth, the doctrine should emphasise transparency as a constitutional expectation in the design and operation of public-sector data systems. As a matter of principle, individuals should be able to know, at least in general terms, which categories of their data are shared, between which agencies, for what purposes, and under what legal authority. Current practice under the Data Sharing Act 2025 does not clearly guarantee systematic public reporting on the scale, frequency, and types of inter-agency data exchanges. Under a doctrine of informational autonomy, opacity would be treated as a factor that counts against the constitutionality of extensive data-sharing arrangements, especially where they significantly affect liberty or equality interests (Abdul Hadi, 2024).
 - v. **Accountability and Redress** - Fifth, the doctrine should require that individuals have accessible avenues to challenge unlawful or disproportionate State data practices, this does not necessarily require a new constitutional remedy, but it does require that existing mechanisms, such as judicial review, constitutional litigation, or complaints to oversight bodies, be meaningfully available in data-related cases. The presence or absence of independent oversight, whether judicial or institutional. Would be a key consideration in assessing whether public-sector data governance is compatible with Article 5(1) and 8(1) of Federal Constitution (Che Yussoff, 2021).

5.3. Application to the Data Sharing Act 2025

Applying this proposed doctrine to the Data Sharing Act 2025 highlights specific areas where constitutional alignment appears fragile. From the perspective of autonomy and justification, the Act's broad definition of "data" and the absence of an explicit distinction between personal and non-personal data mean that very wide categories of personal information can be brought within inter-agency sharing regimes without tailored safeguards. Under a doctrine of informational autonomy, courts could interpret Article 5 (1) as requiring that data-sharing decisions affecting intimate or highly sensitive information be subjected to closer scrutiny than decisions involving aggregated or anonymised data (Daud. M, 2025).

Proportionality concerns arise where inter-agency access is granted on a wide, ongoing basis, with limited temporal or categorical constraints, especially if the same policy outcomes could be achieved with more targeted or pseudonymised datasets. Transparency is implicated by the largely internal nature of the DSA 2025 mechanisms, which make it difficult for individuals to trace how their personal data move through the public sector.

A doctrine of informational autonomy would support interpretations of the Act that favour publication of general data-sharing frameworks, regular reporting, and, where feasible, mechanisms enabling individuals to obtain information about significant uses of their data. In the absence of constitutional litigation on the Act, it remains uncertain how Malaysian courts would respond to a challenge framed explicitly in terms of informational autonomy. Nonetheless, the doctrine provides a

structured lens through which courts could evaluate whether specific applications of the DSA 2025 unduly impair personal liberty or equality.

6. CONCLUSION

The proposed doctrine of informational autonomy could be developed in Malaysia through at least three complementary pathways: judicial interpretation, legislative reform, and institutional design. First, courts could, in appropriate cases, explicitly recognise that certain dimensions of personal data control fall within the protective scope of Article 5(1), drawing analogies from existing liberty and dignity jurisprudence.

Such recognition could be incremental, starting with cases involving particularly intrusive or wide-ranging public-sector data practices, rather than attempting to define a comprehensive right in a single judgment. Secondly, the Parliament could revise or supplement the Data Sharing Act 2025 and related statutes to incorporate explicit references to constitutional principles of autonomy, proportionality, and non-arbitrariness, thereby operationalising the doctrine in positive law. This might include introducing public-sector data protection provisions, mandating privacy impact assessments, and imposing heightened safeguards for sensitive categories of data.

Thirdly, institutional reforms, such as strengthening existing bodies or creating a specialised oversight mechanism for government data practices which could give practical effect to accountability and redress dimensions of informational autonomy. These pathways are not mutually exclusive; together, they would help embed informational autonomy as a living constitutional principle guiding Malaysia's digital transformation, rather than as a purely theoretical construct.

REFERENCES

- A.Halim, N., M.Yusof, Z., Mat Zin, NA., (2018) The Requirement for Information Governance Policy Framework in the Malaysian Public Sector, *International Journal of Engineering & Technology*, p 236.
- Alibeigi, A., & Munir, A. B. (2020). Malaysian personal data protection act, a mysterious application. *U. Bologna L. Rev.*, 5, 362.
- Alibeigi, A., Munir, A. B., & Karim, M. E. (2019). Right to privacy, a complicated concept to review. *A Complicated Concept to Review*.
- Alibeigi, A., Munir, A. B., & Karim, M. E. (2021). Right to Privacy, a Review of Definition, Theoretical Aspects and Development. *Alibeigi, A., Munir, AB, & Karim, MD (2021). Right to Privacy, a Review of Definition, Theoretical Aspects and Development [E-book]. Published, 05-25.*
- Bari, A. & Shuaib, FS (2009). Constitution of Malaysia: Text and Commentary, *Pearson Malaysia*, 3rd Ed.
- Che Yusoff SF& Nordin R, (2021) Freedom of Expression in Malaysia: Compatibility with the International Human Rights Standard, *Besstur*, E-ISSN 2722-4708 Vol.9 August 2021, p 34-42.

- Daud, M. (2025). A Legal Framework for Public Sector Data Sharing in Malaysia: The Clash Between Data Protection, Privacy and Public Interest. *IIUM Law Journal*, 33(2), 279-320.
- Desrochers, P. R. (2024). Access to Information and Privacy: Practical Approaches for Public Service Reform. *Canadian Public Administration*, 67(4), 562-572.
- Gstrein, O. J. (2023). Data autonomy: Recalibrating strategic autonomy and digital sovereignty. *European Foreign Affairs Review*, 28(4).
- Hamid, N. A., Salleh, K., Harun, N., & Bidin, A. (2019). Erosion of the concept of constitutional supremacy in Malaysia. *International Journal*, 4(15), 27-35.
- Harun, Q. N. (2025). Menilai semula kedaulatan data Malaysia: Kritikan struktural terhadap Akta Perkongsian Data 2025: Reassessing Malaysia's data sovereignty: A structural critique of the Data Sharing Act 2025. *International Journal of Interdisciplinary and Strategic Studies*, 6(10), 631-657.
- Hashim, N. (2020). Right to privacy and malaysian practice: a step further in recognising another aspect of human Rights. *Environment-Behaviour Proceedings Journal*, 5(SI3), 289-295.
- Islam, M. T., Munir, A. B., & Karim, M. E. (2021). Revisiting the right to privacy in the digital age: A quest to strengthen the Malaysian data protection regime. *JMCL*, 48, 49.
- Islam, M. T., Sahula, M., & Karim, M. E. (2022). Understanding GDPR: Its legal implications and relevance to South Asian privacy regimes. *Islam, MT, Sahula, M., & Karim, ME (2022). Understanding GDPR: Its Legal Implications and Relevance to South Asian Privacy Regimes. UUM Journal of Legal Studies*, 13(1), 45-76.
- Khairul Anuar Abdul Hadi, Rohana Abdul Rahman & Zainal Amin Ayub. (2024). Freedom of information in Malaysia: International legal instruments and restrictions under National Law. *UUM Journal of Legal Studies*, 15(1), 221-247.
- Legido-Quigley, C., Wewer Albrechtsen, N. J., Bæk Blond, M., Corrales Compagnucci, M., Ernst, M., Herrgård, M. J., ... & Sulek, K. (2025). Data sharing restrictions are hampering precision health in the European Union. *Nature Medicine*, 31(2), 360-361.
- Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, 2025(1), 5536763.
- Malaysia- Overview on the Data Sharing Act 2025, <https://conventuslaw.com/report/malaysia-overview-on-the-data-sharing-act-2025/>
- Nisar, M. A., & Muhammad, S. A. (2025). Privacy as a Legal Right: A Comparative Study Between Pakistan and Malaysia. *JOURNAL OF ARTS AND LINGUISTICS STUDIES Ученумену: Mega Institute for Advance Research and Development*, 3(1), 839-858.
- Ong, B.J., (2020), Proportionality in Malaysia: New Dawn or 'Merely Obiter'?, Chapter 5ed, Cambridge University Press.
- Roßnagel, A., & Richter, P. (2025). Big Data and Informational Self-Determination. Regulative Approaches in Germany: The Case of Police and Intelligence Agencies.
- Shuaib, FS (2023) The Constitution and Human Rights: Revisiting the Constitution of Tan Sri Haun M Hashim, *IIUM Law Journal Vol 31*, Pg 43
- Sukerta, P. A. D., & Sutrisno, A. (2024). Personal Data Protection in ASEAN: A Critical Comparison between Indonesia's and Malaysia's Legal Frameworks. *Constitutional Law Review*, 133-147.

- Sweet, AS & Mathews, J, (2017), Proportionality and Rights Protection in Asia: Hong Kong, Malaysia, South Korea, Taiwan – Whither Singapore?, SAcLJ Vol 29.
- Trusted Digital Identity for Secure Online Verification. <https://www.digital-id.my/en>
- Vladimirovna, T. E. (2022). The Right to Informational Self-Determination: On the Edge of Public and Private. *Legal Issues in the digital Age*, (4), 33-51.
- What is MySejahtera, https://mysejahtera.malaysia.gov.my/faq_en/
- What is Pangkalan Data Utama (PADU) , <https://padu.gov.my/soalan-lazim>
- Widiarto, A. E., Hassan, M. S., Rusli, M. H. M., & Setiawan, E. B. (2025). The authority relationship of Central and Local Governments in forming laws and regulations: between Indonesia and Malaysia. *Legality: Jurnal Ilmiah Hukum*, 33(1), 148-167.
- Zhao, H., Cui, X., & Li Y. (2025). Protecting Malaysia's Technological Autonomy: Innovative Governance Frameworks to Counter Digital Hegemonies. *Journal of Asia Social Science Practice*, 1(1), 112-129.
- Zulhuda, S. (2002). *Personal Data Protection in the Cyberspace: A Comparative Study* (Doctoral dissertation, Ahmad Ibrahim Kulliyah of Laws, International Islamic University Malaysia).
- Zulhuda, S. (2013). Right to Privacy: Development Cases and Commentaries. *Constitutional Law and Human Rights in Malaysia-Topical Issues and Perspectives*. Selangor: Thomson Reuters Malaysia Sdn. Bhd.